(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 199 19 909 C 2**

(51) Int. Cl.[7]:
H 04 L 9/00
G 07 C 9/00

(21) Aktenzeichen: 199 19 909.4-31
(22) Anmeldetag: 30. 4. 1999
(43) Offenlegungstag: 2. 11. 2000
(45) Veröffentlichungstag der Patenterteilung: 19. 7. 2001

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Wincor Nixdorf GmbH & Co. KG, 33106 Paderborn, DE

(72) Erfinder:
Nolte, Michael, 33034 Brakel, DE

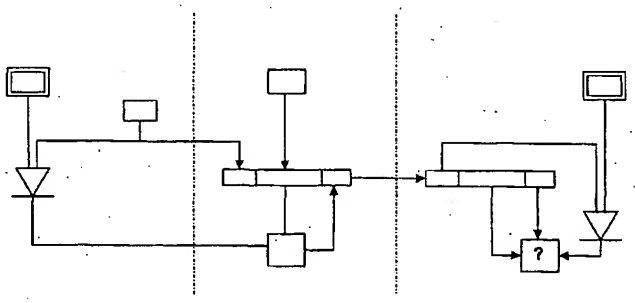
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 197 18 547 A1
US 57 68 385
US 57 54 656
US 45 49 075
EP 08 04 003 A2

BEUTELSPACHER, A. u.a.: Chipkarten als Sicherheitswerkzeug, Berlin, Springer-Verlag, 1991, S. 69-71;

(54) Signierung und Signaturprüfung von Nachrichten

(57) Verfahren zur Signierung einer Nachricht (22) durch einen Absender (20) und Prüfung der Signatur durch einen Empfänger, wobei eine Zentrale (10) und ein Empfänger (30) über einen geheimen gemeinsamen Hauptschlüssel (11, 11') verfügen, mit den Merkmalen:
- Die Zentrale (10)
- erzeugt eine Sequenzzahl (12) und
- aus dieser unter Verwendung des Hauptschlüssels (11) mittels einer Einweg-Verschlüsslung (13) einen Signierschlüssel (14) und
- stellt dem Absender den Signierschlüssel (14) bereit;
- der Absender (20)
- bildet mittels des Signierschlüssels (14) eine Signatur (22c) über die Nachricht (21, 22b) und
- sendet an den Empfänger einen Nachrichtensatz (22), der zumindest die Nachricht (22b) und die Signatur (22c), enthält.
- Der Empfänger (30)
- bestimmt die Sequenzzahl (22a'),
- bildet den mittels der Einweg-Verschlüsslung (13') und dem Hauptschlüssel (11') einen Prüfschlüssel (14') und
- prüft damit die Signatur (22c) der Nachricht.



DE 199 19 909 C 2

DE 199 19 909 C 2

Beschreibung

Technisches Gebiet

Die Erfindung betrifft die Signierung und Singnaturprüfung von Nachrichten unter Verwendung geheimer Schlüssel.

Stand der Technik

Für die Fälschungssicherung von Nachrichten ist bekannt, daß mit Hilfe von symmetrischer Kryptographie eine Signatur gebildet wird, mittels derer der Empfänger mit sehr hoher Wahrscheinlichkeit prüfen kann, ob die Nachricht unverfälscht übermittelt wurde und von dem vorgegebenen Absender stammt. Voraussetzung ist jedoch, daß Absender und Empfänger über einen gemeinsamen geheimen Schlüssel verfügen, der sicher gespeichert sein muß. Ein solches Verfahren ist beispielsweise in der Patenschrift US 4,549,075 beschrieben.

Symmetrische Kryptographie, insbesondere das DES-Verfahren, wird häufig in Chipkarten eingesetzt, weil es sehr effizient programmierbar ist. Die Chipkarten weisen ferner einen Permanentspeicher auf, in dem ein Hauptschlüssel sicher geheim gespeichert ist, der auch in einer Zentrale sicher gespeichert ist.

Soll nun eine Nachricht fälschungsgesichert von einem Absender an den Empfänger, hier die Chipkarte, gesendet werden, so muß bislang der Absender die Nachricht von der Zentrale signieren lassen, da die Zentrale den geheimen Hauptschlüssel nicht dem Absender zur Verfügung stellen kann, ohne das Gesamtsystem zu schwächen. Zudem sind Maßnahmen notwendig, damit die Nachricht bei der Übertragung von dem Absender zur Hauptstelle gegen Verfälschung und Vortäuschung eines legitimen Absenders geschützt ist.

In der Patentschrift US 5,754,656 wird ein Verfahren dargestellt, bei dem eine Nachricht, die von einem Terminal **10** erzeugt wird, von einer Chipkarte **20** mit einem ersten Schlüsselpaar K(A, C) signiert wird, dann zu einem Hostrechner **40** geschickt, dort entschlüsselt, mit einem zweiten Schlüsselpaar K(B, C) neu verschlüsselt und dann dem Rechner **30** geschickt wird. Hierbei handelt es sich um eine bekannte Umschlüsslung, bei der die zu signierende Nachricht an eine Zentrale geschickt werden muß, die einen mit dem vorgesehenen Empfänger gemeinsamen geheimen Schlüssel hat.

In den Patentanmeldung EP 0 804 003 A2 und DE 197 18 547 A1 werden Signaturverfahren mit asymmetrischen ('public key') Algorithmen beschrieben, die per se keine gemeinsamen Hauptschlüssel benötigen, aber erheblich rechenaufwendiger sind als die symmetrischen ('private key') Verfahren.

In der Patentschrift US 5,768,385 und in der Veröffentlichung "Beutelspacher, A., u. a., Chipkarten als Sicherheitswerkzeug, Berlin **1991**, S. 96–71" wird die Signatur wiederum durch eine Zentrale geprüft.

Aufgabe der Erfindung ist es daher, ein Verfahren zur Fälschungssicherung von Nachrichten durch eine Signatur anzugeben, die von einem Absender gebildet und zu einem Empfänger gesendet werden kann, ohne daß der Absender über den geheimen Hauptschlüssel verfügt, den der Empfänger und eine Zentrale gemeinsam haben, oder die Nachricht zuvor zu der Zentrale zwecks Signaturbildung gesendet werden muß.

Darstellung der Erfindung

Die Erfindung benutzt ein Verfahren, bei dem die Zentrale Signierschlüssel vorab bildet und dem Absender bereitstellt. Der Empfänger kann, wie genauer in den Ausführungsbeispielen beschrieben wird, den Signierschlüssel nachbilden und damit die Nachricht prüfen.

Es handelt sich um ein Verfahren zur Signierung einer Nachricht, wobei eine Zentrale und der Empfänger einen permanenten gemeinsamen Hauptschlüssel haben. Die Zentrale erzeugt vorab eine Sequenzzahl und aus dieser mittels einer Einwegfunktion einen Signierschlüssel. Beides wird gesichert dem Absender bereitstellt. Der Absender bildet mittels des Signierschlüssels eine Signatur der Nachricht und sendet sie mit Sequenzzahl und Nachricht an den Empfänger. Der Empfänger bildet mittels Einwegfunktion, Hauptschlüssel und Sequenzzahl einen Prüfschlüssel und prüft damit die Signatur der Nachricht.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung, welche in Verbindung mit den beigefügten Zeichnung die Erfindung an Hand eines Ausführungsbeispiels erläutert.

Kurzbeschreibung der Zeichnung

Es zeigt

Fig. 1 ein Diagramm, in dem der Datenfluß mit den beteiligten Komponenten symbolisiert ist.

Beschreibung mindestens einer Ausführungsform mindestens der Erfindung

In **Fig.** 1 sind die drei Teilnehmer an dem Verfahren, nämlich die Zentrale **10**, der Absender **20** und der Empfänger **30**, durch punktstrichlierte Linien getrennt, angedeutet.

Die Zentrale **10** enthält einen gesicherten Speicher **11** für einen geheimen Schlüssel, der ansonsten beispielsweise in einem symmetrischen kryptographischen Verschlüsslungs- oder Signierverfahren verwendet wird. Der Empfänger **30** enthält einen entsprechenden Speicher **11'**, der denselben Schlüssel enthält. Das Einschreiben dieses Schlüssels erfolgt beispielsweise in der Zentrale bei der Initialisierung, wenn es sich bei dem Empfänger **30** um eine Chipkarte handelt. Andernfalls sind aus der Kryptographie bekannte Schlüsselverteilungsverfahren anzuwenden. Dabei wird der Schlüssel nur einmal oder in sehr großen Zeitabständen gespeichert; für das Verfahren nach der Erfindung ist die Speicherung als permanent anzusehen.

Die Zentrale **10** enthält ferner einen Sequenzgenerator **12**. Dieser liefert eine Reihe von jeweils unterschiedlichen Zahlen. Im einfachsten Fall ist dies eine fortlaufende Nummer. Besser ist jedoch die Verwendung eines bekannten Pseudo-Zufallszahlengenerators, z. B. nach der Modulo-Methode. Bei richtiger Wahl der Parameter liefern diese Pseudo-Zufallszahlen-Generatoren eine Folge von jeweils neuen Zahlen, bis der durch den Modulus bestimmte Zyklus durchlaufen ist. Auch können absteigende Nummern oder solche mit einer Schrittweite größer als Eins verwendet werden. Gleichfalls möglich ist die Verwendung von Datum und Uhrzeit als eindeutig Sequenznummer, gegebenenfalls als Zahl der Sekunden seit einem verabredeten Beginn.

Die Zentrale erzeugt also ein oder mehrere Sequenznummern **12**. Aus einer solchen Sequenznummer **12** wird mittels des Hauptschlüssels durch einen Einweg-Verschlüssler **13** ein Signierschlüssel **14** gebildet. Dies geschieht am einfachsten, indem die Sequenznummer **12** mittels des Hauptschlüssels verschlüsselt wird. Hierbei wird eine kurze Sequenznummer durch weitere Daten auf die Blocklänge des

Verschlüsslungsverfahrens aufgefüllt. Zwar sind hierzu binäre Nullen verwendbar; besser ist eine Funktion der Sequenznummer, z. B. deren Quadrat. Auch möglich ist ein konstanter Text, der nicht aus binären Nullen besteht und vertraulich gehalten wird. Da meist die Blockgröße in der Größenordnung der Schlüssellänge liegt, ist das Ergebnis als Schlüssel weiterverwendbar; gegebenfalls sind Bits aufzufüllen oder durch Faltung die Bitzahl zu reduzieren.

Wesentliche Eigenschaft des Einweg-Verschlüsslers ist es, daß ein Rückschluß auf den Hauptschlüssel praktisch nicht möglich ist. Obwohl die soeben beschriebene Methode keine Einweg-Verschlüsslung ist, weil z. B. der Empfänger durch Dechiffriern aus dem Signierschlüssel die Sequenzzahl bilden könnte, ist die "Einweg"-Funktionalität wesentlich.

Daher werden in anderen Ausführungsformen andere Einweg-Funktion verwendet, die Hauptschlüssel und Sequenznummer reproduzierbar zu einem Signierschlüssel verknüpfen, ohne daß jemand ohne den Hauptschlüssel zu einer gegebenen Sequenznummer einen gültigen Signierschlüssel bzw. umgekehrt bilden oder aus dem Signierschlüssel und der Sequenznummer den Hauptschlüssel bestimmen kann. Solche Verfahren werden allgemein als "Message Authentication Codes" (MAC) bezeichnet. Ein solcher kann insbesondere durch eine beliebige, kryptographisch sichere Einweg-Funktion auf eine Kombination von Hauptschlüssel und Sequenznummer gebildet werden. Als Kombination sind u. a. Konkatenation, Exklusiv-Oder, Multiplikation mit oder ohne Modulobildung, Addition möglich.

Die Zentrale **10** stellt also ein oder mehrere Paare von Sequenznummer **12** und daraus erzeugtem Signierschlüssel **14** bereit. Dies kann z. B. Ausdrucken auf Sicherheitspapier, durch Einspeichern in eine weitere Chipkarte oder durch sonstige gesicherte Datenübermittlung geschehen. Diese Paare werden dem Absender **20** vorab zur Verfügung gestellt und müssen von diesem gesichert und vertraulich gespeichert werden.

Der Absender **20**, der eine Nachricht **21** an den Empfänger **30** senden möchte, entnimmt ein Paar von Sequenznummer **12** und Signierschlüssel **14** und bestimmt die Signatur der Nachricht **21** mittels des Signieres **24**. Bevorzugt wird auch hierbei das DES-Verfahren, z. B. nach ANSI X9.9, verwendet. Alternativ kann eine Signatur durch eine Kombination einer kryptographischen Hash-Funktion mit einem "message authentication code" erzeugt werden. Verfahren hierzu sind in der kryptographischen Literatur vielfach und ausführlich beschrieben.

Sodann bildet der Absender eine Datensatz **22**, der drei Felder mit der Sequenznummer **22a**, der Nachricht **22b** und der Signatur **22c** enthält. Der soeben verwendete Signierschlüssel **14** wird gelöscht.

Nunmehr wird der Datensatz **22** zu dem Empfänger **30** überträgen, welcher damit einen Datensatz **22'** erhält, der wiederum drei Felder enthält, die als Sequenznummer **22a'**, Nachricht **22b'** und Signatur **22c'** angesehen werden. Üblicherweise wird dieser Datensatz bereits von anderen Sicherungs- oder Plausibilitäts-Mechanismen gegen Übertragungsfehler gesichert.

Der Empfänger extrahiert aus dem empfangenen Datensatz **22'** die Sequenznummer **22a'** und führt diese zusammen mit dem Hauptschlüssel **11'** einer Einweg-Verschlüsslung **13'** zu, die dieselbe wie die Einweg-Verschlüsslung **13** in der Zentrale **10** bzw. dazu funktionsgleich ist. Am Ausgang der Einweg-Funktion entsteht ein Prüfschlüssel **14'**. Dieser ist, wenn die Sequenznummer korrekt übertragen wurde, gleich dem Signierschlüssel **14**, den der Absender **20** verwendet hat. Der Prüfschlüssel **14'** wird zusammen mit der eingetroffenen Nachricht **22b'** und der eingetroffenen Signatur **22c'** einem Signaturprüfer **38** zugeführt wird. Passen alle drei zueinander, erzeugt der Signaturprüfer **38** an seinem Ausgang ein Freigabesignal für die Weiterverwendung der Nachricht. Der Prüfschlüssel **14'** wird, unabhängig von dem Ergebnis, mit Abschluß der Prüfung vernichtet.

In einer Weiterbildung der Erfindung führt der Empfänger eine Liste bereits benutzter Sequenzzahlen und weist Nachrichten mit bereits verwendeten Sequenzzahlen ab. Damit ist eine zusätzliche Sicherheit gegen Mißbrauch gegeben.

Da die die Sequenzzahl bevorzugt durch einen deterministischen Generator erzeugt wird, kann die Übermittlung der Sequenzzahl entfallen. Da ohnehin der gemeinsame Hauptschlüssel in gesicherter Umgebung an den Empfänger übertragen werden muß, kann zugleich der Anfangswert des Generators übertragen werden. Mit jeder empfangenen Nachricht erzeugt der Empfänger einen neuen Wert für die Sequenzzahl und bildet damit den Prüfschlüssel **14'**, ohne daß die Sequenzzahl mit übertragen werden muß. Um robust gegenüber Doppelübertragungen und verlorene Nachrichten zu sein, wird dann zweckmäßig auch einer der letzten und folgenden Sequenzahlen mit verwendet werden. Auch hier kann die Zentrale dem Absender mehrere Signierschlüssel **14** bereitstellen, die dann vom Absender in der vorgegebenen Reihenfolge verwendet werden sollen.

Eine mögliche Anwendung der Erfindung liegt auf dem Gebiet der Geldausgabeautomaten. Die Zentrale ist dabei die Bankenzentrale, die für die Prüfung der PIN einen Hauptschlüssel verwendet und an den Hersteller von Geldautomaten in der Zentrale personalisierte Prüfmoduln liefert. Als Absender kommt ein Hersteller oder eine lokale Bankenorgansation in Betracht, die beispielsweise einen Umrechnungskurs oder einen Rabattsatz in den Geldausgabeautmaten laden möchte; aber weder einen eigenen geheimen Schlüssel in den Geldautomaten einbrigen kann noch einen eigenen Sicherheitsmodul einbauen möchte.

Falls kein nichtflüchtiger Speicher im Empfänger vorhanden ist, kann der Empfänger auch die Sequenzzahlen von Anfang erzeugen und mit jeder die Signatur verproben. Der Verlust an Sicherheit ist dabei gering, jedoch ist keine Sicherhiet gegen Doppelbenutzung gegeben.

Patentansprüche

1. Verfahren zur Signierung einer Nachricht (**22**) durch einen Absender (**20**) und Prüfung der Signatur durch einen Empfänger, wobei eine Zentrale (**10**) und ein Empfänger (**30**) über einen geheimen gemeinsamen Hauptschlüssel (**11, 11'**) verfügen, mit den Merkmalen:
   - Die Zentrale (**10**)
   - erzeugt eine Sequenzzahl (**12**) und
   - aus dieser unter Verwendung des Hauptschlüssels (**11**) mittels einer Einweg-Verschlüsslung (**13**) einen Signierschlüssel (**14**) und
   - stellt dem Absender den Signierschlüssel (**14**) bereit;
   - der Absender (**20**)
   - bildet mittels des Signierschlüssels (**14**) eine Signatur (**22c**) über die Nachricht (**21, 22b**) und
   - sendet an den Empfänger einen Nachrichtensatz (**22**), der zumindest die Nachricht (**22b**) und die Signatur (**22c**), enthält.
   - Der Empfänger (**30**)
   - bestimmt die Sequenzzahl (**22a'**),
   - bildet den mittels der Einweg-Verschlüsslung (**13'**) und dem Hauptschlüssel (**11'**) einen Prüfschlüssel (**14'**) und
   - prüft damit die Signatur (**22c**) der Nachricht.

2. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12, 22a, 22a') zusammen mit dem Signierschlüssel (14) von der Zentrale an den Absender (20) übergeben und von diesem über den Datensatz (22, 22') an den Empfänger übergeben wird.

3. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12) durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Empfänger erzeugt wird.

4. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12) durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Absender erzeugt und über den Datensatz (22, 22') an den Empfänger übergeben wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Sequenzzahl durch einen Generator für Pseudo-Zufallszahlen erzeugt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei als Einweg-Verschlüsslung die Verschlüsselung der Sequenzzahl mittels des Hauptschlüssels verwendet wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Zentrale (10) vorab mehrere Signierschlüssel (14) erzeugt und diese, ggf. gemeinsam mit den zugehörigen Sequenzzahlen (12), an den Absender (30) übermittelt.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Empfänger (30) eine Liste bereits verwendeter Sequenzzahlen führt und bereits verwendete Sequenzzahlen abweist.

9. Einrichtung zur Signierung einer Nachricht (22, 22'), die von einem Absender (20) an einen Empfänger (30) geschickt wird, mit den Merkmalen:

- Eine Zentrale (10) und der Empfänger (30) verfügen über einen ersten und zweiten Speicher für einen geheimen gemeinsamen Hauptschlüssel (11, 11');
- in der Zentrale (10) ist ein erster Einweg-Verschlüssler (13) an einem Eingang mit dem ersten geschützten Speicher (11), an einem anderen Eingang mit einem Generator (12) für eine Sequenzzahl verbunden,
- der Ausgang des Einweg-Verschlüsslers (13) ist über ein Transportmedium mit dem Absender (20) verbunden,
- beim Absender ist ein Signatur-Generator (24) vorgesehen, dessen Eingänge mit dem Ausgang des Einweg-Verschlüsslers und der zu signierenden Nachricht (21, 22b) verbunden sind,
- der Ausgang des Signatur-Generators (24) ist mit einer Einrichtung verbunden, die mindestens die Signatur (22c) und die Nachricht (22b) zu einem Nachrichtenblock (22) assembliert und deren Ausgang über ein Transportmedium mit dem Empfänger (30) verbunden ist,
- im Empfänger ist ein Signatur-Prüfer (38) vorgesehen, an dessen Eingänge einerseits mit der Nachricht (22b') und der Signatur (22c') des über das Transportmedium eingetroffenen Nachrichtenblocks (22'),
- andererseits mit dem Ausgang eines zweiten Einweg-Verschlüsslers (13') verbunden ist, dessen Eingänge einerseits mit dem zweiten Speicher (11') für den geheimen Hauptschlüssel und mit einem Mittel zur Bereitstellung einer Sequenznummer (22a') verbunden ist.

10. Einrichtung nach Anspruch 9, wobei ein Generator die Sequenzzahl (22a') nach einem deterministischen Verfahren ein oder meherere Sequenzzahlen entsprechend der Anzahl der Prüfungen erzeugt.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 199 19 909 C2
Int. Cl.[7]: H 04 L 9/00
Veröffentlichungstag: 19. Juli 2001

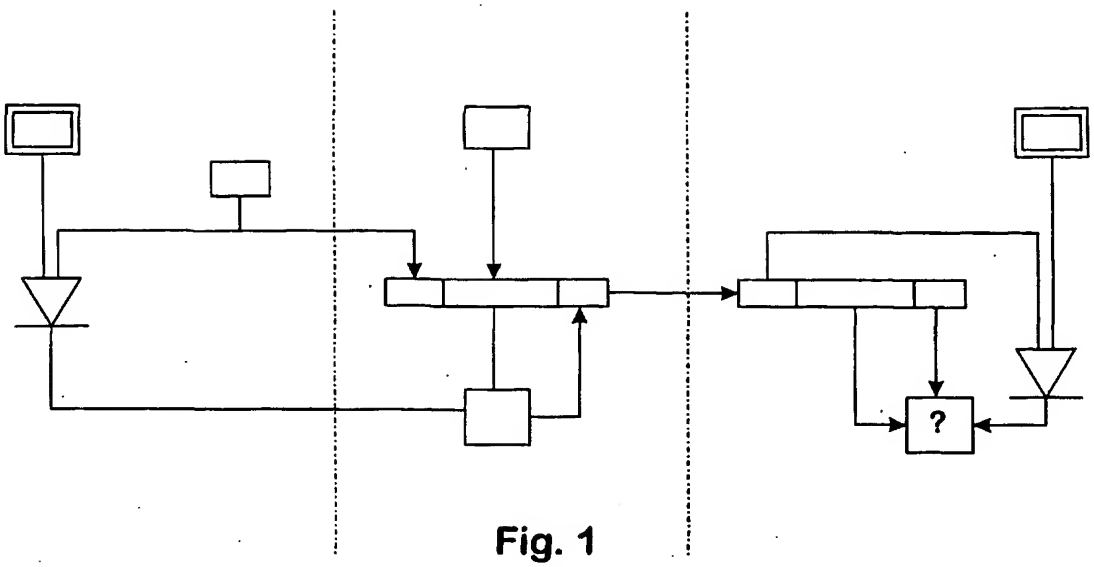


Fig. 1